REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED

4. TITLE AND SUBTITLE

START MAKING SENSE: MANAGING THE COMMAND'S INFORMATION (U)

5. FUNDING NUMBERS

6. AUTHOR(S)

MAJ DAVID B. PISTOLI, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

SCHOOL OF ADVANCED MILITARY STUDIES
ATTN: ATZL-SWV
FORT LEAVENWORTH, KANSAS 66027-6900
COM 913-758-3301 DSN 720-3301

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION UNLIMITED

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

SEE ATTACHED

14. SUBJECT TERMS

INFORMATION MANAGEMENT
INFORMATION OPERATIONS
INFORMATION FAILURE
FRICTION

15. NUMBER OF PAGES
52

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to *stay within the lines* to meet *optical scanning requirements*.

Block 1. Agency Use Only *(Leave blank)*.

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

C	- Contract	PR	- Project
G	- Grant	TA	- Task
PE	- Program Element	WU	- Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. *(If known)*

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

DOD	- See DoDD 5230.24, "Distribution Statements on Technical Documents."
DOE	- See authorities.
NASA	- See Handbook NHB 2200.2.
NTIS	- Leave blank.

Block 12b. Distribution Code.

DOD	- Leave blank.
DOE	- Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.
NASA	- Leave blank.
NTIS	- Leave blank.

Block 13. Abstract. Include a brief *(Maximum 200 words)* factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code *(NTIS only)*.

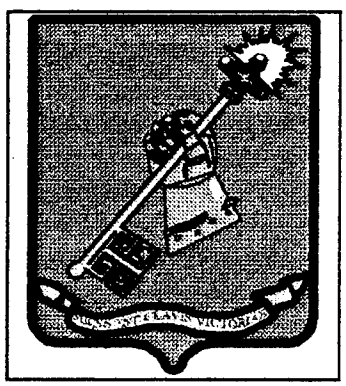
Blocks 17. - 19. Security Classifications. Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

START MAKING SENSE
Managing The Command's Information

A Monograph
by

Major David B. Pistilli
United States Air Force



School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

First Term AY 94-95

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major David B. Pistilli

Title of Monograph: Start Making Sense: Managing the Command's Information

Approved by:

Robert M. Epstein, Ph.D. — Monograph Director

COL Gregory Fontenot, MA, MMAS — Director, School of Advanced Military Studies

Philip J. Brookes, Ph.D. — Director, Graduate Degree Program

Accepted this 17th day of December 1995

ABSTRACT

START MAKING SENSE: MANAGING THE COMMAND'S INFORMATION
by Major David B. Pistilli, USAF, 54 pages.

The purpose of this monograph was to illuminate *information* as both a resource and a process that deserves structured, coherent management at the unit level. The thesis is that lack of such management contributes to needless friction that degrades a unit's ability to perform its mission.

The monograph qualifies information as a resource, examines the importance of information to a military organization, and defines five "information failures" -- insufficient, overabundant, irrelevant, inaccurate, and untimely information -- that disrupt a unit's decision and execution cycles. The Scud-hunting efforts during Operation DESERT STORM are analyzed for examples of delay and mistakes caused by friction due to information failures. The monograph then proposes a framework for managing information as a traditional, tangible resource and process. It further highlights nontraditional properties of information relevant to a 21st century force.

The monograph recommends the creation of an information officer position on the commander's staff, similar to a chief information officer in organizations outside the military. This officer would be coequal to the other officers who manage resources and processes on the commander's staff today -- S/G/J1 through S/G/J8. The role of this officer would be to bring unity to what is now a disjointed effort to manage the command's information. This officer is not envisioned as a technocrat but someone who would blend mission, process management, and information technology expertise to assure the unit uses its information to its best tactical, strategic, and organizational benefit.

The monograph is conceptual rather than procedural or technical. It takes a technological-independent approach that addresses frustration with a wide array of technologies that promise efficiency and effectiveness but consume extra effort in their operation. With increasing emphasis on information technologies, the information on which they are based needs to be well-understood to improve the results from investment in these technologies. The end state sought is a unit where information lubricates rather than impedes mission accomplishment.

TABLE OF CONTENTS

Introduction

Knowledge is power -- Francis Bacon[1]

An abundant but elusive asset stands in line to be counted by today's leader and manager as a resource worthy of oversight. That resource is information.

Information about one's enemy has long been a sought-after commodity by military professionals. Indeed, information about one's rival is a natural consequence of anyone locked in competitive struggle. Thus, intelligence establishments have flourished to formalize the process of collecting, analyzing, and presenting information about an enemy to military decision-makers and executors. Today's US Army specifically, and the military in general, has codified this process into the "combat function" of "Intelligence".[2] A career military intelligence officer on the commander's staff is responsible for the performance of this combat function in the planning and execution of battle. He presides over many formal sub-processes to accomplish this function, and may have a small staff himself. He is the staff proponent for presenting information about an enemy to his commander and the rest of the staff.

Similarly, the commander organizes formal staff sections to oversee other processes critical to the functioning of his unit, both in peacetime and in battle. A personnel officer oversees the administration of people. An operations officer has charge of constructing and executing the combat or other "business" of the unit. (For example, the operations officer of a communications unit would supervise, and be responsible for, the provision of communications by members of his unit.) A logistician supplies and maintains the unit with everything from food and water to commercially-procured equipment. On larger and joint staffs, professionals in formal sections manage standing combat plans and long term programs that affect the unit or command, and career

communicators are dedicated to managing the telecommunications and automation of the command. Special staff members are added to administer, among many other matters, civil-military relations, political affairs, public affairs, legal matters, science and technology, money, facilities, history, and official complaints.[3]

The currency -- the medium of exchange -- of most, if not all, of these staff processes is information. The players in these processes traffic information to accomplish their tasks. Very few actually execute -- pull a trigger, drive a vehicle, repair a weapon. Yet, for all of this traffic, the information itself is rarely organized as a resource, one with intrinsic value and one that requires management oversight as both a resource and a process. Without such oversight, the information is frequently wasted -- either misspent or not used.

One obstacle to categorizing information as a resource is its overpowering intangible characteristic. Tangibly, one can record data -- even knowledge -- in books, manuals, standard operating procedures, reports, logs, and recordings. The collection can have many formats: paper, magnetic, optical. Yet, much data and knowledge is intangible -- that kept by people in their brains. Perhaps more importantly, this intangible information affects the very manner by which people organize tangible information. Each military occupation -- and individuals within the same occupation -- organize information to suit their character. This is natural and desirable to a certain degree but it presents a standardization and interoperability issue we frequently choose not to address because it infringes on people's autonomy. Moreover, it influences the dichotomy between tangibility and intangibility toward the latter. Thus, unlike a tangible resource -- people, money, facilities, or equipment -- the dichotomous resource, information, has no unifying staff proponent and is left unmanaged.

Because of this dichotomous nature and without a staff proponent, the commander has little way to accurately or efficiently monitor information flow and accuracy. Information flow is itself a process -- really, many processes -- yet it is only dimly acknowledged and rarely codified. There are notable exceptions, such as the broadcast of an Emergency Action Message or the nine line forward air controller briefing to an attack aircraft.[4] These are normally at the extreme end of the spear, and for good reason: a standardized procedure and format saves lives in combat.

Most information flow, though, is ephemeral, accomplished often without a trace. Unlike the processes of operations, planning, maintenance, training, security, and supply, all of which have staff proponents charged with their oversight, information management falls between the commander, his chief of staff, his executive officer, his signals officer, and his administrative staff. When it does receive peripheral acknowledgement as a process -- in the combat function of Battle Command, as command and control communications[5] -- the unlucky proponent, normally the XO, must untangle and wrestle an incongruent web of people, procedures, and systems to allow the commander the use of information to "orchestrate men and things toward performing their missions in war."[6] Without dedicated attention to information as a resource, and to its flow as a process, this orchestration frequently seems more a cacophony than a symphony.

Such discordance imposes a toll on the unit in the form of friction. This friction I shall call "information failure." I define information failure as inefficiencies or breakdowns in other processes due to insufficient, overabundant, irrelevant, false, or untimely information. The failure either contributes to human error or requires special effort to overcome. This friction, at its low end, can simply consume extra resource, either in time spent

searching for correct information to make the right decision, or by resource misspent through the wrong decision. At its high end, this friction can be fatal; for example, an artillery officer may incorrectly assess friendly fire acquired by a targeting battery as that of an enemy and fire a counter-battery mission on a friendly unit. In almost all cases, information failure is reducible, if not avoidable, if information flow is properly managed.

There is a further toll imposed by information failure that transcends simply compartmenting pieces of information properly or having just the right amount to make a decision. This toll is that of an organization unable to properly use its corporate knowledge to accomplish its mission. A commander presides, essentially, over an immense mountain of knowledge -- his own, his staff's, and the individual knowledge of each member of his command. Like an iceberg, the vast bulk of this knowledge lies beneath the visible surface of a unit. Each person has a specific knowledge of his primary responsibility, his expertise. This expertise is constantly shared or executed, laterally and vertically, inside and outside the unit. It also waxes and wanes, individually and corporately, dependent on recency of use as well as on physical constraints such as permanent or temporary assignments, leaves, illnesses, even death on the battlefield. The accumulation and transfer of this knowledge can be monumentally inefficient and extraordinarily capricious. As a commander, one must have two goals. First, one must build and preserve corporate knowledge for consistent unit performance. Second, one must assure that knowledge transfer -- the exchange of information, inside and outside the unit -- gets the right information, to the right place, to the right person or system, at the right time to accomplish a job correctly. Only by so doing can the commander receive the best return on this currency of his command, information.

This paper, then, will explore information management and flow in a military unit to answer seven primary questions. First, what is information? Second, what makes it a resource? Third, of what value is information to a military? Fourth, why is it worthy of special oversight? Fifth, how can information "fail" a unit and present friction? Sixth, how can a unit prevent or restrict information failures? Finally, can a special proponent for information on the commander's staff make the difference? The answers to these questions should illuminate how best to harness and wield information for the commander.

What Is Information?

> Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information? -- T. S. Eliot[7]
>
> Where is the information we have lost in data? -- Harlan Cleveland[8]
>
> Webster's Third New International Dictionary defines information as:
>
> ...Knowledge...communicated by others or obtained from investigation, study, or instruction;...knowledge of a particular event or situation: intelligence, news, advices;...facts or figures ready for communication or use as distinguished from those incorporated in a formally organized branch of knowledge: data;...a signal (as one of the digits of a telephone number) purposefully impressed upon the input of a communications system or a calculating machine...[9]

The definition expresses multiple concepts that encompass current use of the word: knowledge, intelligence, communication, study, instruction, news, facts, figures, data.

A useful model that incorporates the totality of what "information" has come to mean is a "knowledge spectrum" where "data, information, knowledge, and wisdom can be viewed as part of continuum, one leading into another, each the result of actions on the preceding, with no clear boundaries between them."[10] The spectrum is represented below.

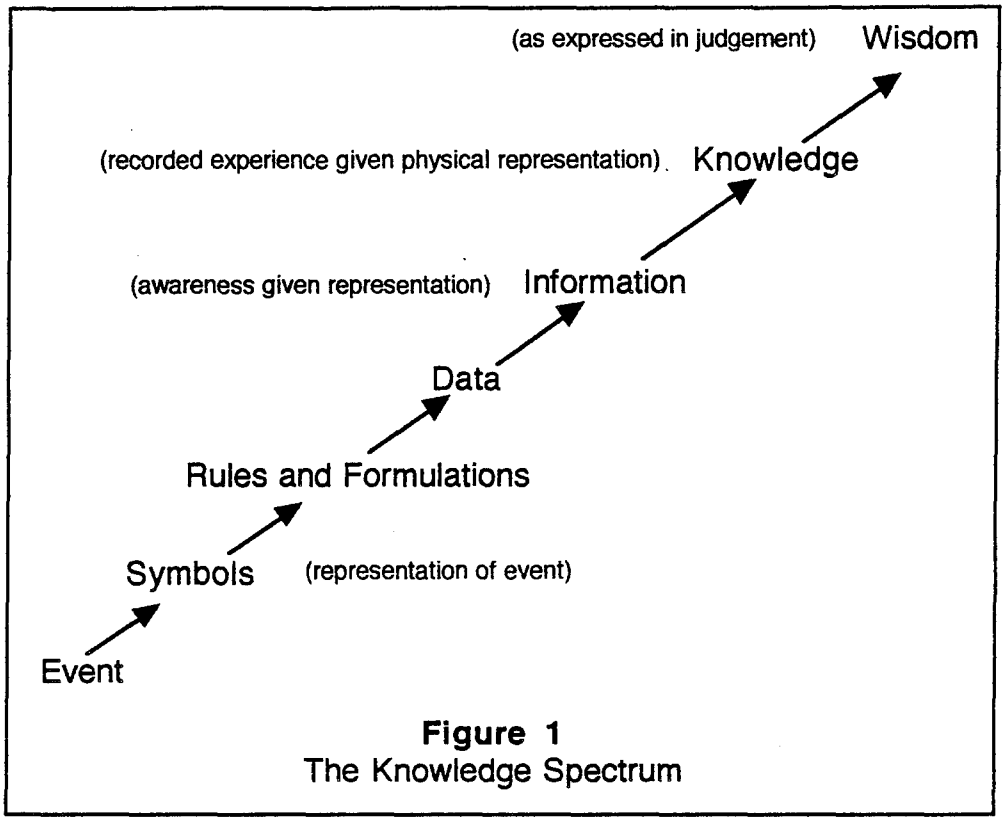


Figure 1
The Knowledge Spectrum

From Anthony Debons, Esther Horne, and Scott Cronenweth, Information Science: An Integrated View (Boston, Massachusetts: G.K. Hall and Company, 1988), 5.

The continuum is important for two reasons. First, it comprises four constructs basic to a non-scientific use of the term "information": data, information (the word itself!), knowledge, and wisdom. Second, it represents these concepts fluidly, hierarchically but not rigidly, in the manner of common use. Their meanings are listed below for clarity.[11]

> *Data:* Letters, numbers, lines, graphs, and symbols, etc, used to represent events and their state, organized according to formal rules and conventions. An example of data for a fighter pilot would be radar contacts on his surveillance display.
>
> *Information:* The cognitive state of awareness (as being informed) given representation in physical form (data). This physical representation facilitates the process of knowing. To extend the above example, were an AWACS controller to advise the pilot, "Three groups -- First group north bullseye 8 heading east; second group southwest bullseye 5 heading east; third group marshaling west bullseye 15,"[12] the pilot would be informed about what those contacts mean -- in this case, numbers, range, bearing, and activity.

Knowledge: The cognitive state beyond awareness. Knowledge implies an active involvement and understanding and the ability to extend the level of understanding to meet life's contingencies. Knowledge can also refer to the organized record of human experience given physical representation (books, reports). In our fighter pilot example, he brings the knowledge of friendly and enemy capabilities and tactics and uses this knowledge to decide how to conduct his engagement.

Wisdom: Implies the application of knowledge...centered around certain criteria or values that are generally accepted by the culture or society. For our fighter pilot, this could be the use of his knowledge, derived from education, training, and experience, to organize and operate his unit or plan for battle.

This holistic definition of information captures most concepts intended by current use of "information", especially for the military.

What Makes Information A Resource?

> There's a war out there...a world war. And it's not about who's got the most bullets. It's about who controls the information...it's all about the information! -- Phil Alden Robinson[13]

One senses intuitively that information thus defined is quantifiable, qualifiable, and possesses some value. In other words, it has the characteristics of a resource. A resource is the "available means (as of a country or business); computable wealth (as in money, property, products); immediate and possible sources of revenue <rich natural resources>..."[14] Information qualifies as a resource on all counts.

First, information can itself be a means to an end. Joint Pub 0-1 lists information as an *instrument* of national power.[15] Instruments of national power are defined as "employable" and "represent tangible resources that can be purposefully crafted, manipulated, altered, and balanced."[16]

Second, information can be viewed as an asset -- the property or product -- of an organization. A library is an example of an organization in which the bulk of its value resides in its holdings, as well as its ability to connect to or

gather even more information than exists physically on its premise. A "news-gathering service such as the Associated Press"[17] is an example of an organization whose sole output is information in the strictest sense of the word. A news program such as National Public Radio's *All Things Considered* produces information throughout the depth of our earlier definition: data, information, knowledge, even wisdom.

Third (and this blends with the concept of a resource as an asset), information can be a source of revenue. Dictionaries, encyclopedias, and source-books all derive income for their authors and publishers. A publishing house markets the accumulated knowledge of thousands of authors.[18] A bookstore retails the products of many publishers. Such revenue need not derive solely from the printed word, moreover. "Management consulting firms" sell both very specific and very broad expertise -- knowledge -- to the customer who does not have either the manpower or skill to acquire and process information for himself.[19]

What Is The Value Of Information To The Military?

> It is a truth beyond argument that full and accurate information becomes most vital at the point of impact, for unless it is correctly applied there, the wisest plans of the ablest generals will fail. -- S. L. A. Marshall[20]

While such definitions focus on an economic character of information as a resource, and economics will certainly play a role in the efficiency proper information management can bring to a unit, information is a resource of greater dimension for the military. Specifically, information derives value from the ability it gives a military to understand its tactical, strategic, and organizational environment.

Tactically, information is a valuable resource for the knowledge it builds about the friendly force, its physical and intellectual environment, and its

adversary. Information about the force itself generally relates to capability. This includes current strength and health of both people and equipment. It includes the ability to sustain a force logistically, the tactical logistics functions of "manning, arming, fueling, fixing, moving, and sustaining soldiers and their systems."[21] It includes a unit's training proficiency in specific mission-essential tasks. It includes a unit's ability to synchronize and support a commander's scheme of maneuver through intelligence, fires, protection, signals, and engineering. Finally, it includes an assessment of a unit's will. To assemble such information is no mean feat, and a commander organizes his staff to apprise him of status across the spectrum of battlefield operating systems. The commander makes decisions about feasible courses of action for his force based on a thorough understanding of all these elements, for they comprise his unit's combat capability. No modern commander would -- or should -- embark on a mission without such knowledge.

Information about the physical environment includes descriptions and analyses of the terrain, climate, and people in the area of operations. Terrain dominates the information we seek about a region and comprises the topography of a location as well as analysis of its characteristic features. This analysis is formalized to include observation, cover and concealment, obstacles, key terrain, and avenues of approach -- "OCOKA" in the parlance of ground units.[22] Meteorologic history and forecast prepares a unit for the weather it will face and analysis of the impact it will have on operations. The demographics of a region freezes a statistical snapshot of the people and points to the beginnings of understanding the intellectual environment a unit will enter.

Information about the intellectual environment has two components. The first is the manner in which our superiors frame the tactical event. This framework includes the commander's intent, the mission's purpose, method,

and end-state, and the concept of operations. These are so important they compose, in concise and distinct format, paragraphs two and three of a standard five paragraph field order.[23] Rules of engagement are also information about our superior's view of the event. The second component of the intellectual environment is a knowledge of the culture of a people as well as an understanding of the underlying causes of a conflict in the region of the tactical event. This knowledge bridges raw statistical information -- the demographics -- with the final tactical value of information: knowledge of an adversary.

Information about an enemy is the Holy Grail for military forces and the primary reason for existence of an entire military specialty, Intelligence. Unlike his counterpart staff officers, who advise the commander on the status and abilities of their individual soldiers and systems, the intelligence officer must also advise the commander on the way his threat thinks and might act. As such, he has perhaps the most formalized system in the military for managing information. He plans and directs the intelligence effort, collects information, processes the information, and produces and disseminates intelligence that commanders, other decision-makers, and executers will understand.[24] As with the knowledge of his own force, a modern commander seeks as much information as possible about his adversary. Indeed, this can be so consuming that the commander must be prudent enough to narrow his focus and prioritize the intelligence effort for his staff.

Taken together, information about friendly forces, the physical and intellectual environment, and an adversary has tactical value for a military force. The qualification of this value, and the advantage it confers, is relative to the extent that a commander can shape an information battle space that

maximizes this information for a friendly force and minimizes the same for an adversary.

Strategically, information is a valuable resource for the knowledge it builds about the context within which the military operates and the future it faces. The context includes extranational dynamics such as regional threats, alliances, and US interests abroad. It also includes domestic dynamics such as national interests and objectives, economics, and politics.[25] The military, in a democratic society, uses this information to define virtually every aspect of itself: size, structure, skills, facilities, equipments, technologies, doctrines. Decisions made without such information would be meaningless and culpable. Further, a military must extrapolate from such present information to posture itself for future operations. Although more difficult to derive than tactical information -- it involves considerable application of knowledges and large amounts of raw information to arrive at an increased and accurate knowledge of the strategic setting -- strategic information can possess proportionately greater value. Qualifying this value is relative to the accuracy of the raw information and multiple analysts' understanding of the forces that shape the strategic setting -- today, tomorrow, and twenty years from now.

Organizationally, information is a valuable resource for the knowledge it builds and holds about a military's nature, about its "product", and, more mundanely, about it administration. "Nature" here means an organization's character, tradition, and reason for existence. The military as a profession is moderately unique in imbuing its soldiers, sailors airmen, and marines -- its "employees" -- with the tenets and realities of the profession: duty, honor, integrity, loyalty, service. These tenets were not created spontaneously or in a vacuum; they developed from experience over the course of centuries. Educating young troops, and refreshing old ones, requires knowledge of these

experiences in order to apply them today. Perhaps more than any profession, the military relies on the knowledge of its history to understand its nature today.

In much the same way, the "products" of a military are built from the information of those who went before. These deliverables range from occupational skills, such as medicine, construction, or communications, to gross corporate missions, such as war fighting or peacekeeping. Again, the military is relatively unique in that it accesses untrained individuals and then teaches technical occupational knowledge. It further assembles specific numbers of various occupations in a unit in order to accomplish a broader mission. These individual knowledges accrue to become a corporate knowledge, both for a unit and for the larger service and military. Formally and informally, units and individuals communicate across different boundaries to learn from others' experiences. As the learning matures, it broadens into doctrine and is taught to a new generation of learners. Just as we derive principles of war, fundamentals of offense or defense, or operational art from study of warfare since recorded history, so will the lessons learned from today's operations be the information that feeds tomorrow's doctrine, tactics, techniques, and procedures.

Finally, information both fuels and lubricates the administration of an organization. Whether information is that assembled to allow a decision to be made or that collected to conduct a finance or personnel transaction, information feeds the process. More subtly, information can smooth a process. Primarily, this information assumes the form of knowledge of one's environment. Knowledge of one's commander's intent and unit mission orients individual action in the right direction and frees the individual from worry about performing at cross-purpose to his teammates or his boss. Knowledge of a specific procedure to follow in conducting an action guides efficient, proper accomplishment of that action. Knowledge of a specific procedure to follow in

coordinating an action -- that is, communicating information to others -- reduces frictions in a system as a whole and assures better corporate knowledge. Commanders intuitively sense this when they push general situational knowledge down the chain, understanding that their troops' emotional comfort depends, in part, on their knowledge of their environment. The more comfortable they are, and the more they know about higher intent, the better they will perform.

To sum up, information accrues tactical value for the knowledge it conveys about the friendly force, about the physical and intellectual environment within which that force operates, and about the adversary that opposes it. It accrues strategic value for the knowledge it conveys about the global context within which it might be used. Finally, it accrues organizational value for the knowledge it conveys, builds, and nurtures on the nature of the military, on the "know-how" of a force, and on the procedures that comprise any system.

Does Information Require Special Oversight?

> In a knowledge society, the [leader's] effective power is the product of his formal power multiplied by his knowledge competence. If he is near zero in either factor he will have little effective power. -- Dale E. Zand[26]

Were these values insufficient to dedicate oversight for information as both a resource and a process, three additional factors will converge to force its coherent management: efficiency, accuracy, and the dominating informational nature of future war.

Efficiency is the "ability to produce a desired effect...with a minimum of effort, expense, or waste."[27] It can be measured physically as output divided by input. The concept of efficiency is embodied in the now proverbial "Do more with less." The harried military professional, already working impossibly hard,

responds: "I can only do less with less." While few would question the vigor of a military's work, and no one intentionally wastes effort or expense, information can be a lever that increases the ratio of output to input.

The primary necessity for such efficiency is a decreasing -- in real terms -- military budget. The American taxpayer will find it increasingly difficult to dedicate roughly 250 billion dollars of the nation's annual revenue and one million of its citizens to an active duty defense force. Inefficiencies -- many of which currently exist in administrative information management -- will have to be weeded out to preserve output given dwindling input. An example of one such effort, currently underway, is Corporate Information Management (CIM).

CIM seeks simply to standardize and consolidate the information methodologies and systems that manage the "business" functions of the Department of Defense: accounting, finance, personnel, contracting, procurement, supply, and so forth. The concept makes sense: administering these functions, and their information, should not be so drastically different between military services that they require separate procedures and systems. Yet such separateness exists today, born not from a malicious intent to be different but simply from an institution that did not manage information, and its systems, as a coherent whole. While there remains some dispute over the dollar savings CIM can ultimately realize, it seems intuitive to understand that CIM represents a real efficiency that levers information to preserve capability while sparing resource.

A second necessity for efficiency is the continually growing focus on joint and combined military action. Such action can be a recipe for inefficiency: separate services and nations bring separate cultures, methods, and equipments to the fight. Separateness is desirable when it provides distinctive

force tools that can be skillfully blended to achieve a synergy. However, this separateness can also cause wasteful effort, expense, even interference.

One example was the Desert Shield/Desert Storm Air Tasking Order (ATO). When the US Air Force developed a process and the equipment to develop and distribute the ATO and the US Navy -- for good or bad reasons, or a combination of the two -- developed a separate system, one service could only coordinate with the other through special means. During Desert Shield and Desert Storm, for example, the Navy flew both a paper and a computer diskette version of the daily ATO to its fleet from the Joint Forces Air Component Commander headquarters in Riyadh, Saudi Arabia.[28] Even then, the Navy lacked the information management system -- the Computer-Assisted Force Management System -- to manipulate the unwieldy ("telephone book"-sized[29]) document for individual units to extract the information germane to them.

Coherent information management smooths, rather than impedes, this process. Action taken during peacetime to develop interoperable communications systems, common sensing/shooting systems, and standard procedures is integrative at the precise time it needs to be: during armed conflict when different services and nations come together to conduct military action.[30]

Accuracy is related to, but distinct from, efficiency. It is "the quality or state of being...free from mistakes or errors; precise."[31] Accuracy is certainly one component of efficiency. Yet, it implies more. In a sentence, it means "...being at the right place at the right time with the right capabilities."[32] An honorable goal for good information itself, coherent information management is vital to two components of this definition: strategic mobility and lethality/survivability.

Strategic mobility is a characteristic of an increasingly continental US-based force that faces a world-wide, dynamically defined threat. Such a force, because it might have to fight its way into a theater,[33] can not afford to be the wrong force for the mission. It can not afford to arrive in the wrong order. It can not afford to have supplies arrive later than it does, or arrive at the wrong locations. Such a force has to be accurate from the start.

Such a force also has to be credibly lethal and survivable. Lethal because it is our ability to impose our will on an adversary that makes the use of force a viable policy option. Survivable because as a smaller, better but less densely equipped, and less deeply sustained force, its people, weapons, and supplies -- as always but now acutely so -- are precious.

Information will allow the mobility, lethality, and survivability the force requires in the form of intelligence, in the form of the leaders' vision of their battlespace, and in subordinates' ability to effect that battlespace accurately. Proper information on an adversary should assure development of the proper plan to deal with the contingency. This will help build the leader's understanding of friendly and enemy force capabilities and his vision of how the force will dominate an adversary through fire and maneuver.[34] It will allow the tailoring, equipping, and rehearsing of that force for the capabilities and knowledge the force needs to execute on the battlefield. Last, it will allow the assembly of lift that moves the force where it needs to be, when it needs to be there.

Finally, the informational nature of future war will demand unique oversight of information. Two complementary concepts will contribute to this requirement: knowledge-based operations and information operations.

Knowledge-based operations are those operations where "situational knowledge"[35] -- and the authority to act upon that knowledge -- are diffused

throughout the organization. The knowledge will consist of a complex combination formed from the campaign plan, operations order(s), fresh intelligence, and responsive targeting information. The diffused knowledge will be made possible through a "non hierarchical dissemination of [this information] at all levels."[36]

Basing an operation on knowledge of plans, orders, intelligence, and targets is certainly not new. Indeed, this knowledge forms the substance of the combat decision-making process used today to construct an operations order. What will be new is the manner by which the knowledge that forms the order is accumulated, disseminated, and updated. The new process will not have information flow downhill into pipes of ever-decreasing size until only a trickle runs out at the operator level. The new process will be "internetted" rather than the hierarchy we are accustomed to today.[37]

Complementing knowledge-based operations will be information operations. Information operations are those

> ...that enable, enhance, and protect the commander's decision cycle and execution while influencing an opponent's...through effective intelligence, command and control, and command and control warfare...supported by all available friendly information systems...[38]

Again, this concept is not new -- the Army has long recognized command and control as a function or system operating on the battlefield,[39] and the Air Force is oriented, much as in aerial combat, toward "turning inside" an adversary's decision "loop."[40] What is new is recognition of the power of and reliance on *information* as a crucial element in combat power dynamics.[41] It is integral to the processes that comprise accurate and effective maneuver, firepower, protection, and leadership.

As an operation, a focus on information can maximize those processes as well as highlight the previously murky combat over the *means* of and

capability to command and control. This combat -- "command and control warfare" --will integrate physical destruction, electronic warfare, operations security, military deception, and psychological operations to counter an adversary's command and control and protect friendly C2.[42] Such combat, always a feature of war and in the future more coherently so, is the most visible and attractive feature of an information focus. There will have to be more mundane attention, though, that fully maximizes combat and non-combat processes. This attention will have to root-out big and small information inefficiencies in the daily business of a unit.

How Does Information "Fail" The Unit?

> Everything in war is very simple, but the simplest thing is difficult. The difficulties accumulate and end by producing a kind of friction that is inconceivable unless one has experienced war. -- Carl von Clausewitz[43]

Information fails the unit when it contributes to the inefficiency or breakdown in other processes -- combat and non-combat -- due to its insufficiency, overabundance, irrelevance, inaccuracy, or untimeliness. Short definitions follow.

Insufficient information is a real or perceived shortage of the information an individual or group requires to accomplish a task. The condition of insufficient information may exist during a general shortage of information, such as when a unit is cut-off from its parent or sister units. It can also exist in a general information glut, when every manner of information abounds except what is needed. A common example is intelligence streaming in from collection points on every avenue except that on which an adversary chooses to advance.

Overabundant information is the converse of insufficient. It is more information than required to accomplish a task. Again, it can be either real or

perceived. It is a common complaint today and presents perhaps the most insidious friction -- it appears benevolent but saps energy at a frightening pace.

Irrelevant information is that not needed to accomplish a task. The condition of irrelevant information can exist during either shortages or overloads -- it simply occurs when an information process has not been accurately designed to collect, process, and transmit the correct information. Briefings and reports, whether short or long, scarce or plentiful, are famous for irrelevance.

Inaccurate information is false. It can be a mistake such as the mistranscription of an order or report, or the misinterpretation of the same when the order or report is repeated verbally. It can be exaggeration, as is the wont when describing physical action in combat. It can be rumor or opinion instead of fact. Finally, it may be deliberate, part of a friendly or enemy deception.

Untimely information is that whose usefulness has expired. It might have been sufficient, relevant, and accurate but was not transmitted or presented when needed. Knowledge of enemy intent for what transpired yesterday has far less use today than knowledge of enemy intent for what is planned tomorrow.

These failures produce a friction that hinders both the unit's ability to decide and the ability to execute. The ability to decide or execute generates from well-understood, well-practiced procedures coupled with sufficient, relevant, accurate, timely information. Poor information, or poor information processes, can cripple one half of this equation.

Information fails the decision or execution by causing delay or mistake. Delay can result from seeking additional information when a real or perceived information shortage exists. It can result from the sorting through of too much information, or irrelevant information, to find the crucial pieces. It can result from initially planning a poor course of action based on inaccurate information, or in time spent verifying and correcting accidentally or deliberately false information.

In all cases, the correct decision or execution is slowed as the correct information is sought.

If the correct information can not be found, or there is not the time or inclination to find it, a bad decision can be made or faulty course followed. Like a delay, a mistake can stem from the friction presented by the information half of the procedure + information equation.

Delay and mistake in deciding and acting, due to poor information, occur daily in peacetime. A commander will never truly know how well his unit supports his customers unless he solicits feedback, or if the only feedback he receives is from irate customers. A technician with outdated or no repair manuals either can not repair his equipment, or does so incorrectly. A rumor about leadership, pay, leave, work conditions, alluring but false, permeates the unit to decrease mission accomplishment or leader credibility.

In war, delay and mistake are often aggravated by combat, sometimes with lethal result. A commander might wait too long to commit his reserve, denied current information from the fight or hoping for more accurate information to better steer this force. He might commit the force too soon, or in the wrong manner. Supplies may be ordered too late or sent to the wrong point by logisticians unable to track battlefield consumption, dooming an attack to culmination or a defense to penetration. A tank gunner may incorrectly assess a thermal image of a friendly vehicle in his sight as that of an enemy and shoot it.

The effort to seek and destroy Iraqi surface-to-surface missiles during Desert Storm encapsulates these delays and mistakes due to information-induced friction. Insufficient, inaccurate, or untimely information contributed to late or poor decision and execution.

One *delayed decision* was that of employing American special forces as an element of the mini-campaign against the Iraqi Scuds. Major General Wayne A. Downing, commander of the Joint Special Operations Command, first proposed use of his forces to combat the Scud launches on 22 January 1991.[44] Coalition offensive air operations against Iraq had started on 17 January; the first Iraqi Scuds had been launched against Saudi Arabia and Israel on 18 January.[45] Yet the decision to use MG Downing's forces did not occur until 30 January.[46]

One of the contributing reasons for this delay was insufficient and inaccurate information with which to make a decision. Foremost, the depth and breadth of Iraqi Scud resources was not fully known. While American planners had accounted for fixed launcher sites during the initial phase of the attack, they were subsequently confronted with a fleet of elusive mobile launchers.[47] The size, launch sites, and dispersed logistics locations for this fleet of mobile launchers was not anticipated and never adequately discerned. Without an appreciation for the extent of the threat, initial force levels and activity to counter the Scuds was considered adequate by the US Central Command (USCENTCOM) planners. They would soon have to amend that decision, throwing not only MG Downing's special forces but triple the number of aircraft as originally planned into the fray as well.[48]

An example of a series of arguably *mistaken decisions* that occurred during the anti-Scud campaign because of information failure were those involving an early F-15E strike against a suspected Scud logistics base, Al Qaim. The mission was diverted from its original target less than six hours before take-off.[49] Normal mission planning by the flight crews had to be condensed; specific targeting data was delivered to the crews literally as they walked to the planes; the time-on-target (TOT) -- critical to the synchronization of

support to the strike package -- changed twice. In the ensuing confusion, not all required support showed and one aircraft was shot down, its aircrew alive but detained for the duration of the war.

In this instance, information processes were not timely enough to cope with the changed and compressed schedule. The Air Tasking Order (ATO) is a complex choreography of aerial maneuver, intelligence, logistics, fire support, protection, and command and control. Intelligence could not provide sufficient information to the crews soon enough to adequately plan. Fire support, in the form of lethal suppression of enemy air defenses (SEAD) by radar hunter-killer aircraft, never received word of the changed TOT and missed rendezvous with the strike package. Protection, in the form of non-lethal SEAD from electronic combat aircraft, was driven off by an Iraqi attack; this information was not passed to the flying mission commander. Denied this knowledge, the mission commander chose to press the attack when he may well have diverted or aborted had he known the strength of Iraqi air defenses and the weakness of his own position. Similarly, the Combat Operations Squadron of the Air Operations Center, charged with prosecuting the current air battle, either overtly decided or unwittingly did not decide to delay or abort the mission. These decisions (or indecisions) may well have been different had sufficient, accurate, timely information flowed to either decision-maker.

The anti-Scud campaign itself is an example of *delayed execution* due, in part, to informational friction. To the Israeli government and, to a lesser extent, the American government, the CENTCOM effort to suppress and destroy these weapons seemed slow to start and inadequate in total.[50] To CENTCOM, however, their efforts were early and gave the missiles perhaps more attention than they deserved. Fixed Scud launch sites were targeted the first night of the air campaign.[51] Simultaneously, British special forces waged a clandestine

effort against a portion of the Scud launch area in Western Iraq.[52] American special forces would soon follow.[53] Batteries of Patriot surface-to-air missiles would be deployed to Israel.[54] More aircraft would be redirected to the effort later, totaling three squadrons flying 2,500 sorties by war's end.[55] Why the difference in perspective?

Unintentional and deliberate information shortage was part of the problem. Admittedly, CENTCOM underestimated the ubiquity and persistence of the mobile launcher threat and did not anticipate the eventual force that would need to be allocated to it. The result was a lag that allowed the Iraqis to launch 26 Scuds toward Israel,[56] straining Israeli patience with the coalition effort to suppress the launches.

Curiously, the US also withheld information from Israel. While the anti-Scud campaign birthed a veritable information thrash in an effort to keep Israel apprised of the coalition effort -- diplomatic activity was intense and military reporting on "Scud-hunting" seems to have been as burdensome and useful as reporting body counts in Vietnam[57] -- the US elected not to detail American special forces involvement in the campaign, an involvement the Israeli's were especially eager for.[58] Ostensibly for security reasons, this information shortage compounded a tense situation.

One final example, of *mistaken execution* due to information friction, was the frustrating effort to discern true Scud targets. Initial estimates of numbers of mobile launchers -- confirmed after the war by International Atomic Energy Agency personnel -- were between 20 and 30.[59] Yet a combination of US aircrews and special forces reported destroying approximately 90 mobile launchers.[60] Since 19 mobile launchers were known to survive the campaign,[61] one could assume that only approximately ten launchers were truly destroyed; the remaining 80 seem to have been decoys.

This is a case of inaccurate information, in this instance deliberately false information -- decoy Scuds -- promulgated by the Iraqis. In this one example, the Iraqis could be credited with achieving their tactical objective. The Scud attack consumed 2,500 US aircraft sorties, three American special forces units, a British Special Air Service regiment, and six Patriot batteries emplaced in Israel.[62] Unquestionably, these efforts diminished total Scud launches and achieved the greater strategic aim of preventing Israeli retaliation. However, tactically the Iraqis were able to provoke a relatively strong coalition response through their ability to deny the US real information about their mobile launching network and intent.

These delays and errors in decision and execution, induced by the friction of information failures, represent the *effects* of those failures. The *causes* of the failures are twofold: an inability to manage the information resource and an inability to manage the information process.

How Can A Unit Prevent Information Failures?

> Iron will power can overcome this friction; it pulverizes every obstacle but of course it wears down the machine as well. -- Carl von Clausewitz[63]

The answer to the dilemma seems simple: manage the information as a resource and manage the information process. If it were so simple, no failures would exist. The key is to manage information such that it lubricates rather than "wears down the machine."[64] This is a four step process.

The first step is to recognize information as a bona fide resource that deserves unit-level management. One does this intuitively at the personal level: a schedule, a "to-do" list, names and addresses, and so forth. Astute leaders and managers also do this intuitively at the organizational level. For example, the 1st Infantry Division commander appoints his deputy or chief of staff as his "information manager" when the division goes to the field.[65] This person is

responsible for forwarding to the commander, who moves frequently and far around the battlefield, information deemed critical that tends to accumulate in the various operations centers. These are important -- but beginning -- steps.

The second step to managing information as a resource is to apply the same principles as one would apply to tangible things. Today the military -- or any organization -- manages facilities, equipment, supplies, even money by accumulating them, assigning them a value, maintaining them, and securing or safeguarding them. Managing information can, in many respects, be similar.

Information about people can serve as an example. Organizationally and personally, we acquire information constantly, on many different levels. The orderly room accumulates administrative information: name, social security number, rank, and so on. The duty section collects both administrative and capabilities information; one can easily expect to find duplicative administrative information such as names, ranks, and serial numbers but there will usually be more: training status, performance comments, progress toward promotion. The unit commander accumulates all this and more: he will generally know gross numbers of troops in his unit; he will know how these numbers compare to what he is authorized; he will know if he is critically short in numbers, grades, or trained status of a certain skill. Each level or activity in the organization accumulates this information for the same reason they would accumulate any tangible resource: they expect to use it.

As with any asset, the activity assigns a value to the information they collect. Indeed, the value of particular information directs their efforts to accumulate specific pieces of information and not others. The orderly room is charged with the responsibility of collecting all information administrative about the unit's people; thus, they assign priority to it, if they are doing their job correctly. The duty section is interested in elements of this administrative

information but they are charged with more: the responsibility for mission accomplishment by their people, and professional development of their people. Thus, they prioritize management information about capability, readiness, and performance. The commander is interested in this information for all duty sections because he is ultimately responsible for unit mission accomplishment, yet he seeks subtly expanded information: he observes for trends and sharp failures or successes in capability, readiness, and performance. He will direct increased accession or redirect people within the unit; he will focus training efforts; he will resource equipment shortfalls if his people can not maintain proficiency operating or maintaining it. In short, the commander prioritizes information about the people resource.

Each activity maintains that information, even if in the most rudimentary sense. The orderly room neatly files all records, and posts new information to the records as it is received. The duty section similarly files such records but goes one step further: they will review it consistently to better understand their people's progress, or lack of it. The commander alone downloads most maintenance responsibilities to the administrative staff that surrounds him or relies on the duty sections, as well he should: the information he seeks is corporate.

Finally, each activity safeguards the information with which it is entrusted, both physically and intellectually. The orderly room maintains the privacy of individual records and should go to some length to assure the physical integrity of those records against human or natural disaster. The duty section similarly organizes physical files and keeps confidential individual performance records. The commander will not normally expose all management information about his unit, for security and other reasons. Some information is withheld for

operational security, such as gross unit strength; other information is secured to respect the privacy of his people.

The construct of information as tangible resource only takes its management so far, however. Information possesses characteristics different from traditional, tangible resources, characteristics that will dictate both traditional and non-traditional philosophies and methods for managing it. The third step is to recognize these differences and adjust for them. An enumeration of these differences follow.

First, *information is expandable.*[66] Unlike a resource that it is depleted when consumed, information, usually in the form of knowledge, does not decrease in quantity, content, power, or value.[67] Certain information, such as chronological facts about our environment, become less valuable over time. For example, signals intelligence collected two days ago that alerted us to what our enemy did yesterday is less valuable than signals intelligence that will tip us about enemy courses of action tomorrow. Certainly, such information forms a part of our greater knowledge about our adversary, and most such source information is useful historically for the study of war. Yet most information increases with value as it is consumed. In the intelligence example, and using the knowledge spectrum, signals collected represent data. These are organized into factual information by intelligence technicians. Analysts digest the information and process it into a general knowledge about the enemy and our particular situation. This knowledge is presented to the commander who, using prior knowledge and accrued wisdom, makes decisions about how to fight his force. Value is added in each step. Moreover, knowledge of the adversary grew and endures for the commander and his staff.

Second, *information is also compressible.*[68] It "...can be concentrated, integrated, summarized,...miniaturized...for easier handling."[69] "Theorems" and

"formulas" distill the work of great mathematicians and scientists into a universally usable form.[70] Our "nine principles of war"[71] encapsulate experience and study of the subject into a usable framework for our future application. A field manual sums the knowledge of many contributors into one volume for our instruction and reference.[72]

Third, *information is substitutable* for certain physical resources, particularly property, "labor, and capital."[73] An individual who connects via the public switched telephone network to the Internet, which is itself an infrastructure for access to many other networks, need not have a significant office in a specific locale. A portable computer, a modem, and a telephone line will suffice. That same person's ability to tap the different knowledges available on the network obviates the need for employing other individuals whose expertise overlaps that provided by the network. Finally, the information thus accessed is provided by machines operated and maintained by someone else.

Fourth, *information is transportable.*[74] Although investment in the infrastructure can be expensive -- design, construction, upgrade, operation, and maintenance of the computing and distribution systems is the subject of current discussion concerning an "information superhighway" and will represent no mean investment -- the volume of information that will travel it and the speed by which it will travel will dwarf time and space norms of current infrastructures that transport physical resources today.

Fifth, *information is diffusive.*[75] Although it can sometimes be compartmented and controlled in physical form, human nature and information technologies themselves militate against containment. Most information, again, resides in the physical brains of people or virtual brains of machines and resists any jailing. People naturally seek information in their daily lives through human contact, news, and study. Further, people naturally converse; the more

extraordinary the information they possess, the more it seems the information must be communicated and the faster it spreads. Machines, although they make no judgments about the information they possess, divulge it just as readily, and can transfer it far more rapidly. Technology further facilitates the transfer through xerography, telecommunication, signals interception, and computer hacking.[76] Technology can be, and is, used to protect information but there is a delicate tension between technologies that store and transport information, those that secure it, and those that can overcome such security.

Sixth, *information is shareable.*[77] That is, it is not merely exchanged like other resource transactions. Data, information, knowledge, and wisdom are not collected or accrued at the expense of some other element in the spectrum of knowledge; the source information remains intact.

These characteristics: expandability, compressibility, substitutability, transportability, diffusiveness, and shareability put new spin on old management frameworks. Expandable information will require strategies and tactics to accumulate and preserve valued information and discard the less valued. Compressible information will require new thinking on numbers of workers, their locations, and the inventory of information required to sustain them. Transportable information will require infrastructure. Diffusive information helps by spreading knowledge but hurts by spreading secrets, disinformation, and unnecessary information. Finally, shareable information will require new thinking on ownership, value, and accounting for the resource. Information management will progress toward *knowledge* management.

The fourth and final step is to manage the information process. One manages processes by understanding the engine(s) of the process -- how the process works. One must understand the inputs to and outputs from the engine. The engine must have some control mechanism. The process must be made

reliable: simple, understood by all involved, and robust. Finally, the process should be easily maintained if it breaks. Managing an information process is not unlike managing most other processes.

Intelligence information can serve as an example. The engines of information processes -- collection, storage, retrieval, distribution, presentation, and use -- are similar to four of the five steps of the intelligence cycle -- collect, process, produce, disseminate.[78] An intelligence operative or sensor collects information about one or many subject(s). This information must be stored in some form: paper, audio or video tape, computer disk, film. Thus stored, it can be retrieved later by those who need to use it -- processors, analysts, decision makers. The information is distributed physically, either by hand or by electronic transmission. Once distributed it must be presented in meaningful form for those who would use it; this form will be different for different groups of users. The photo processor views raw visual information in a form different from the photo interpreter; the analyst views that information in yet another form; the end customer might see it packaged in a fourth way. At every stage, one or more of the human or automated players in the engine used the information provided to it.

Each step -- each engine -- accepts inputs and provides outputs. The inputs and outputs normally feed some other engine in the chain sequentially, but not always. The collector viewed something and recorded it. Some or all of this recorded information was stored, distributed, and/or retrieved; not necessarily in that order. Thus retrieved or distributed, it was presented and used in some fashion. An effective process has relatively clearly defined inputs and outputs; this allows the engine to be optimized for its function. A human reconnaissance scout, for example, would not seek visual information at night without night vision devices of some sort. Likewise, he would expect to have

the technological and procedural means to transmit his observations: a radio network, cryptography, usable frequency assignments, agreed times for transmission and reception. This definition allows for smooth functioning of the engine.

Each engine has a control mechanism to modulate its function. In the intelligence cycle, the "plan and direct" step is an overarching control for the steps of collecting, processing, producing, and disseminating.[79] Similarly, an information process needs to have its collection effort focused. It needs to be able to contract or expand its storage, respond to differing retrieval requests, and distribute its products in varying ways to meet varying situations. It should be flexible and versatile in its presentation. Finally, if not used, or used differently than intended, it should be drawn down or able to change to accommodate the different use.

The process can not endure an infinite amount of control, however; it must be reliable -- produce the intended output given the intended input -- most of the time. Reliable processes are characterized normally by relative simplicity, understandability, and robustness. Simple processes have higher likelihood of consistent success than complex ones. A simple process contributes to understandability, and an understandable process is an easier process to implement properly than one not easily understood. A robust process -- one that is physically or conceptually sturdy -- resists intentional attack or unintentional failure of certain components in the process.

Processes eventually do fail, but good ones make it easy to pick up the pieces. A process that is modular and has some depth is more easily maintained. With modularity, a non-working component can be replaced without having to replace or repair the entire system supporting the process. With depth, the system can be kept operating, even at reduced levels, while the

broken component is repaired or replaced. Closing with the intelligence model, if the collection plan is redundant or overlapping, one collection asset can fill-in for another if a collection team is compromised or a sensor is destroyed. Another team or sensor, available if there is depth, can be deployed to provide full coverage again.

In summary, information failures and their attendant friction can be avoided or mitigated if information is well-managed as a resource and as a process. In the context of a resource, the information needs to be properly collected, adequately maintained, sufficiently valued, and well protected. In the context of a process, the engines of the process need to be well understood; the inputs and outputs clearly defined; control mechanisms need to be present; the process needs to be reliable in terms of simplicity, understandability, and strength; and the process needs to be easily and quickly repaired if broken.

Since all people manage information in some capacity, these philosophies alone would be almost enough if uniformly applied by everyone in the unit. In an increasingly knowledge-based force, these people would have the aptitude to understand the nature of the information with which they work and the inclination and time to apply sound management to the information resource and information process. Yet, even this will not coherently and most effectively deal with the totality of the information with which the unit decides, operates, and exists.

Can A Special Proponent For Information Help?

Diffused knowledge immortalizes itself. -- Sir James Mackintosh[80]

Every unit, and its commander, needs to have these philosophies embedded uniformly in every core process that accomplishes the mission. Further, the commander needs to have insight into the health of information

management as a resource and management of the information process. One vehicle for accomplishing this is the same as for the management of other resources and other processes: an officer on the commander's primary staff, peer to the S/G/J1 through S/G/J8, charged with these responsibilities. This officer could be called the "Information Officer".

This officer would have the duty, and the authority vested in him by the commander, to assure the unit uses its information resource to its best tactical, strategic, and organizational benefit. The management term of art for this is "Strategic Information Management".[81] "Strategic" here carries many meanings, none solely targeted to the military but useful nonetheless to any organization: using all information means to execute as effectively as possible; assuring operational use of information ties into strategic plans; and integrating new information technologies into a coherent informational and technical architecture that, again, supports strategic plans. The tenets of strategic information management and information engineering provide a four part framework for accomplishing this duty.

First, the information officer would drive an effort to document the "core processes that accomplish the mission."[82] The core processes for a military unit differ between combat and non-combat. The combat functions of intelligence, maneuver, fire support, air defense, mobility and survivability, and battle command comprise the core processes that accomplish the mission while at war or training for war.[83] Peacetime functions that accomplish the mission break down along staff lines: personnel, intelligence, operations and training, maintenance and supply, planning, communications, accounting and finance, and so forth. Documenting these processes demystifies and renders understandable complex functions, themselves consisting of many subprocesses. The documentation would be accomplished primarily by the

"experts"[84] for each function -- maneuver warriors for maneuver, as an example -- with assistance and guidance from the information officer. This documentation will serve as a base line for the way a unit accomplishes its mission now, with current leadership oversight and practices.

Second, the information officer would analyze the processes for "the key decisions that guide mission delivery."[85] One example of this for a portion of the battle command function is the decision support template, a "graphic record of the wargame [that] depicts decision points... associated with movement of forces and the flow of the operation", developed to assist the commander in executing a friendly course of action.[86] This template seeks to synchronize battlefield operating system activity with a command decision based on specific criteria for making the decision. There are more mundane decisions made in garrison, from ordering a part to prioritizing unit spending. Decisions permeate every process, yet the decision information is only half the equation.

Third, the information manager would analyze the processes for the operational information required in each to execute the mission. Execution information completes the information equation. It ranges from the simple to the sophisticated. It can be as mundane as technical orders required by a maintenance technician to repair a piece of equipment, a map of a route for the drivers in a convoy, a diagram of an assembly area for the members of a unit. It can be as exotic as the intelligence imagery from a national collector. It can be conceptual, such as knowledge of the mission and the commander's intent. In any case, it is information the executer needs to turn a wrench, drive a truck, fire a weapon.

Finally, the information officer would architect the means and processes that support those decisions and executions with "the right information to the right people at the right time."[87] This requires a combination of technology and

procedure. Technologically, he would be responsible for assembling the means to "collect, process, and disseminate information in ways that improve [mission accomplishment]."[88] This is the combination of telecommunications and automation that collect, store, retrieve, distribute, and present information. The technical means themselves are not enough, however. It is a truism of computing professionals that automating an inefficient process simply begets automated inefficiency. Procedurally, process documentation and information analysis illuminates procedural and organizational inadequacies and frictions that often can be streamlined without additional technical means.

This documentation, analysis, and technical means integration and oversight would be a significant effectiveness multiplier for any organization, and a combat multiplier for a military unit. For the military, however, the information officer would have one final responsibility: to be the staff director for *information operations*.

Information operations were defined earlier in the paper; essentially, they seek to "gain and maintain the selected, key information the warfighter demands to fight and win, while denying that same information to adversaries."[89] The "components" of information operations are friendly and adversary command and control, command and control warfare (physical destruction, electronic warfare, operations security, military deception, and psychological operations), intelligence, and the "global information environment" (essentially, all other non-defense information systems in the world that can impact the battle environment).[90] With information increasingly viewed as a dynamic of combat power,[91] with the enormous breadth and cross-functionality of information operations (command and control, intelligence, electronic combat, psychological operations), and with the increasing reliance on and subsequent need to protect friendly information systems, the

commander or battle captain should have a synchronizing, expert staff officer to construct and execute the informational element of the total campaign.

This officer will have to blend business expertise (whatever the "business" of that unit is -- ground combat, logistics, communications, medicine, etc.), process management expertise, and information technologies expertise. Ideally, and perhaps eventually, an Information Corps will produce a body of officers with these heady qualifications.[92] However, it is not necessary that the officer have precisely the MOS of the unit he is supporting, or be an automator par excellence. Rather, this officer will have to have a fundamental understanding of the unit mission(s), business analysis, and information technology. He should be the bridge between true experts in these fields, with emphasis on analysis, for it is in the understanding of the processes, information requirements, and information flows that most benefit will derive. He will be the facilitator through which the people who really own the information and the process take ownership for it and use it to the unit's best advantage.

The information officer would best be positioned on the commander's immediate staff, for three reasons. First, strategic information management requires top leadership commitment and authority. The commander's principal subordinates are the primary executors in accomplishing the management of the resource and the process. Their ownership, leadership, and action will be bolstered by a peer who can direct, advise, and assist. Second, strategic information management requires integration across the command to be most effective. An information officer on the commander's staff provides uniform direction to what could be disparate and conflicting efforts. Third, the commander needs both an honest broker he can rely on for guidance and analysis that does not promote an agenda, and a single point of contact for the

planning and execution of information strategies and campaigns. A principal staff officer responsible for information operations, equivalent to the adjutant, intelligence officer, operations officer, logistician, planner, and communicator, would give him leadership, integration, and feedback.

Last, there are some ways the information officer should *not* be viewed. First, he will not be the political officer. His job would not be to tell people or organizations how or what to think. Initiative, innovation, and creativity are prized and necessary for high-performing organizations. Second, he will not be the information "property book custodian". Each activity owns its information and is responsible for managing it. His job is to make sure that information is collected, processed, and disseminated in an integrative and coherent manner to the best advantage of the unit. Third, he will not be solely a technocrat. He will very much be educated on the technology and methodologies of information operations and management but his enduring viewpoint has to be the mission "objectives and plans."[93] Fourth, he will not be the "substitute for institutionalized information management processes."[94] Just as administration, intelligence, operations, supply, and maintenance process success relies on many people working across many functional boundaries to accomplish these missions, so will information operations rely on commitment across functional boundaries to accomplish its mission. Finally, he will not be the emphasizer of control over command.[95] While the addition of another staff officer (and resultant workers) seems to run counter to the notion of streamlining staffs, the information officer is intended to bring order, structure, and vision to that element of the staff and operational environment that everyone complains about but no one seems able to harness: information. His job should simultaneously lubricate the gears of the organization while making its actions more coherent

through efficient and effective information use. The expression of the commander's will should be even clearer and more pronounced.

Conclusion

> The end for which a soldier is recruited, clothed, armed, and trained, the whole object of his sleeping, eating, drinking, and marching is simply that he should fight in the right place at the right time. -- Carl von Clausewitz[96]

Information is a powerful, abundant, and sometimes enigmatic resource, a resource both personal and corporate, tangible and intangible, so ubiquitous that we take its management for granted. Yet, it must be managed if the future force is to most effectively bring friendly knowledge to bear against an adversary.

Information is a word we use loosely, and almost justifiably so: it means many things to many people. For the purposes of this paper, information represents a "knowledge spectrum" consisting of data (representations of events), information (awareness of the data), knowledge (understanding of the data and how to use it), and wisdom (the application of knowledge). This construct comprises four concepts common to a non-scientific use of the term and represents those concepts fluidly.

Information conforms to a traditional view of a resource in that it can be a means, an asset, and a source of revenue. It is a means when it is employed toward an end, such as the informational instrument of national power. It is an asset when it represents the product of an organization, such as the output of an intelligence unit. It can generate revenue when the product is available for sale, either to a payee or as a savings when one unit uses its knowledge to assist another.

Information is a resource of particular value to the military because it helps define a military's tactical, strategic, and organizational environment.

First, we use information to frame the tactical event. This includes information about friendly and adversary capability (strength, health, equipment, sustainability, training, and will), information about the physical environment (terrain, climate, and demographics), and information about the intellectual environment (commander's intent, concept of operations, scheme of maneuver). Second, we use information to understand the strategic context within which we fight. This includes information about domestic dynamics such as national interests and objectives, and supranational dynamics such as regional threats and alliances. Third, we use information to administer ourselves. This administration consists of building and nurturing institutional nature, knowledge, and procedure. It is in this administration that information either fails or assists the unit.

Thus valued, the information resource deserves special oversight if a future force is to be efficient, accurate, and able to compete in the dominating informational nature of war. A decreasing budget is a catalyst for leveraging information to increase output given diminished input. Increasingly joint operations are a catalyst to use information to smooth inherently inefficient action through interoperable communications systems, common sensing/shooting systems, and standard procedures. A strategically mobile force will have to be "...at the right place, at the right time with the right capabilities."[97] Finally, knowledge-based operations and information operations will require close, comprehensive, and expert management of the information resource and process.

When such management is not present, information failures present an irreducible friction, causing inefficiency at best and death at worst. Insufficient, overabundant, irrelevant, inaccurate, and untimely information cause delays and mistakes in decision and execution that consume extra resource of all

types, especially human time and sometimes human life. When such management is present, information failures and their effects can be reduced or avoided entirely.

This management will require committed leadership that first recognizes information as a bona fide resource. Second, this management will have to, as with any tangible resource, accumulate, evaluate, maintain, and safeguard the information resource. Third, information management requires some non-traditional thinking that accounts for its expandability, compressibility, substitutability, transportability, diffusiveness, and shareability. Fourth, management of the information resource will have to include management of its flow -- how the information is acquired, stored, retrieved, distributed, presented, and used.

A special proponent for information will most coherently assure the unit uses its information resource to its best tactical, strategic, and organizational benefit. This "information officer" would combine the tenets of strategic information management and information engineering to manage the information resource and information process. This involves four continuous, overlapping actions: documentation of the "core processes that accomplish the mission", analysis of the processes for "the key decisions that guide mission delivery", that same analysis to illuminate the operational information required in each to execute the mission, and assembling the means and procedures to support those decisions and executions with the "right information to the right people at the right time."[98] This combination of information technologies and information procedures would be established and grow within an architecture that would use information effectively throughout the unit, introduce new technologies and capabilities smartly, and tie tactical and organizational information effort to strategic vision.

The ideal fruition of this concept would be an advantage during conflict as well as peace, but conflict brings an emerging doctrinal duty for the information officer: Information Operations. While the information officer is involved with information operations on a daily basis, a conflict demands control of the information such that the friendly force knows more, knows it sooner, and applies that knowledge more effectively than an adversary. Friendly command and control optimization and protection, command and control warfare, intelligence, and a knowledge of the global non-combatant information players and systems will be the information officer's trade. He will be responsible, essentially, for an "information campaign" within the total campaign.[99]

The information officer will combine a fundamental understanding of his unit's mission, a knowledge of business analysis, and expertise with information technologies to ply his craft. Ideally, this officer will be placed on the commander's principal staff, with the people, leadership commitment, and authority to strategically and coherently manage the unit's information. Finally, this officer will *not* be the political officer, the information property book custodian, the technocrat, or the panacea for all the command's ills. For all the efficiency and control information management might promise, effective command still requires leadership and commitment across functional boundaries.

In the end, if the information officer can help reduce friction in the accumulation, use, and preservation of unit information and knowledge; if he can help steer the iceberg to increased efficiency and accuracy in mission accomplishment by getting the right information, to the right place, to the right person, at the right time; if he can help properly and fully use all unit knowledge; if he help turn what seems a cacophony into a symphony -- then he will have done his duty.

NOTES

[1] John Bartlett, Familiar Quotations, edited by Emily Morrison Beck (Boston, Massachusetts: Little, Brown, and Company, 1980), 158.

[2] Department of the Army, FM 100-5: Operations (Washington, DC: US Government Printing Office, June 1993), 2-12.

[3] Department of Defense, National Defense University, Armed Forces Staff College, AFSC Pub 1: The Joint Staff Officer's Guide 1993 (Norfolk, VA: AFSC, 1993), 2-37 to 2-41. For a description of the responsibilities of the myriad staff positions in a modern army, see Department of the Army, FM 101-5: Command and Control for Commanders and Staff, Final Draft (Fort Leavenworth, KS: US Army Command and General Staff College, August 1993), 3-5 to 3-83.

[4] Department of the Army, FM 90-20/FMFRP 2-72/TACP 50-28, J-Fire: Multi-Service Procedures for the Joint Application of Firepower (Washington, DC: US Government Printing Office, 25 July 1989), 27.

[5] DA, FM 100-5, 2-14 to 2-15.

[6] Martin van Creveld, Command in War (Cambridge, Massachusetts: Harvard University Press, 1985), 16.

[7] Excerpt from T.S. Eliot poem, "The Rock." Cited in Harlan Cleveland, The Knowledge Executive (New York: Truman Talley Books, 1985), 22.

[8] Cleveland, The Knowledge Executive, 22.

[9] Philip Babcock Gove, Editor in Chief, Webster's Third New International Dictionary (United States: G. & C. Merriam Company, 1976), 1160.

[10] Anthony Debons, Esther Horne, Scott Cronenweth, Information Science: An Integrated View (Boston, Massachusetts: G.K. Hall and Company, 1988), 5. This majority view is repeated variously in many texts of information science and management but is not universally accepted, at least by one author. The late Fritz Machlup, a respected information scientist, rejects the definition of "information" as encompassing either "data" or "knowledge." See "What They Mean By Information" in *Semantic Quirks in the Study of Information*, The Study of Information: Interdisciplinary Messages (New York: John Wiley and Sons, 1983), 641-660.

11 Debons, et al, Information Science, 8. The definitions are repeated nearly verbatim; the examples of each using a fighter pilot are those of the monograph author.

12 Weldon B. Shofner, "Was That Tactical or Bullseye, Barnyard?" USAF Weapons Review, Issue 2, Volume 42, (Nellis AFB, Nevada: USAF Weapons School, 1994), 29.

13 From the movie "Sneakers." Cited in HQ USAF/SC briefing on information warfare, 18 Nov 94, slide 2.

14 Gove, Webster's Third New International, 1934.

15 US, Department of Defense, Joint Pub 0-1: Basic National Defense Doctrine (Washington, DC: US Government Printing Office, 1992). Reprinted in US, Department of the Army, Command and General Staff College, C510: Joint and Combined Environments (Fort Leavenworth, KS: USACGSC, 2 Aug 1993), 88.

16 USACGSC, C510, 23.

17 Morton F. Meltzer, Information: The Ultimate Management Resource (New York: AMACOM, 1981), 63.

18 Ibid.

19 Ibid, 64.

20 S.L.A. Marshall, Men Against Fire: The Problem of Battle Command in Future War (Gloucester, Massachusetts: Peter Smith, 1978), 101.

21 DA, FM 100-5, 12-12 to 12-14.

22 Department of the Army, FM 5-100: Engineer Combat Operations (Washington, DC: US Government Printing Office, November 1988), 24.

23 DA, FM 101-5, H-55 to H-59.

24 These actions describe the "intelligence cycle" which depicts a continuous process to satisfy the need for information about an adversary. See Department of the Army, FM 34-1: Intelligence and Electronic Warfare

Operations (Washington, DC: US Government Printing Office, September 1994), 2-15 to 2-17.

[25] The strategic context for the military is well-explained in William J. Clinton, National Security Strategy of Enlargement and Engagement (Washington, DC: US Government Printing Office, July 1994) and Colin L. Powell, The National Military Strategy of the United States (Washington, DC: US Government Printing Office, January 1992).

[26] Dale E. Zand, Information, Organization, and Power (New York: McGraw-Hill Book Company, 1981), x.

[27] David B. Guralnik, Editor in Chief, Webster's New World Dictionary of the American Language (United States: Williams Collins & World Publishing Company, 1978), 445.

[28] Richard P. Hallion, Storm Over Iraq (Washington, DC: Smithsonian Institution Press, 1992), 162, 256.

[29] Ibid, 155.

[30] Martin C. Libicki, The Mesh and the Net (Washington, DC: Institute for National Strategic Studies, National Defense University, 1994), 55.

[31] Guralnik, Webster's New World, 10.

[32] Department of the Army, TRADOC Pamphlet 525-5: Force XXI Operations (Fort Monroe, VA: HQ US Army Training and Doctrine Command, August 1994), 3-1.

[33] James C. Blackwell, lecture to Advanced Military Studies Program, School of Advanced Military Studies, US Army Command and General Staff College (Fort Leavenworth, KS: 12 Dec 94).

[34] DA, TRADOC Pam 525-5, Glossary-1.

[35] Ibid, 2-8.

[36] Ibid.

[37] Ibid.

[38] Ibid, Glossary-4.

[39] DA, FM 100-5, 2-14.

[40] John Boyd; quoted by James Fallows in George E. Orr, Combat Operations C3I: Fundamentals and Interactions (Maxwell AFB, AL: Air University Press, 1983), 19. Thomas P. Coakley also presents this portion of Colonel Boyd's theories. See Command and Control for War and Peace (Washington, DC: National Defense University Press, 1992), 33.

[41] This concept is the force behind the emerging FM 100-6: Information Operations, a US Army doctrinal manual that is one of many efforts focusing attention on the combat potential of information.

[42] See Department of the Army, FM 100-6: Information Operations [Coordinating Draft] (Fort Monroe, VA: HQ US Army Training and Doctrine Command, no date), Chapter 5.

[43] Carl von Clausewitz, On War, translated and edited by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 119.

[44] Rick Atkinson, Crusade: The Untold Story of the Persian Gulf War (Boston/New York: Houghton Mifflin Company, 1993), 140.

[45] Ibid, 509-10.

[46] Ibid, 174-75.

[47] Thomas A Keaney and Eliot A. Cohen, Gulf War Air Power Survey: Summary Report (Washington, DC: US Government Printing Office, 1993), 86.

[48] Atkinson, Crusade, 147.

[49] Information for the facts in the ensuing portion of this paragraph and the following paragraph is derived from Atkinson, Crusade, 124-28; analysis and postulation about decision-making are the monograph author's.

[50] Atkinson, Crusade, 175.

[51] Keaney and Cohen, GWAPS, 17.

[52] Atkinson, Crusade, 142-143.

[53] Ibid, 174-175.

[54] Ibid, 93.

[55] Keaney and Cohen, GWAPS, 84. This 2,500 sortie number counts approximately 1,000 sorties that launched against suspected Scud targets but dropped ordnance on non-Scud targets due to weather, defenses, non-acquisition of primary target, or an even higher priority diversion.

[56] Ibid, 84.

[57] Atkinson, Crusade, 147.

[58] Ibid, 281.

[59] Keaney and Cohen, GWAPS, 87.

[60] Ibid, 83.

[61] Ibid, 87.

[62] Keaney and Cohen, GWAPS, 84; Atkinson, Crusade, 175, 177, 130.

[63] Clausewitz, On War, 119.

[64] Ibid.

[65] Randolph W. House, MG, USA, lecture to Advanced Military Studies Program, School of Advanced Military Studies, US Army Command and General Staff College (Fort Leavenworth, KS: 12 Jan 95).

[66] Cleveland, The Knowledge Executive, 29.

[67] This thought is repeated in many information science and management texts. Meltzer, 60, and Cleveland, 29, assert it most forcefully.

[68] Cleveland, The Knowledge Executive, 31.

69 Ibid.

70 Ibid.

71 See, for example, DA, FM 100-5, 2-4 to 2-6.

72 Cleveland, The Knowledge Executive, 31.

73 Ibid. The subsequent examples are variations of those presented by Cleveland.

74 Ibid, 32.

75 Ibid.

76 Ibid.

77 Ibid, 33.

78 See DA, FM 34-1, 2-15 to 2-17.

79 DA, FM 34-1, 2-15.

80 John Bartlett, Familiar Quotations, edited by Emily Morrison Beck (Boston, Massachusetts: Little, Brown, and Company, 1980), 367.

81 US, General Accounting Office, Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology [GAO/AIMD-94-115] (Washington, DC: General Accounting Office, May 1994), 10.

82 "Establish core processes that accomplish the mission" is the second step of one strategic information management methodology. See USGAO, Executive Guide, 10.

83 DA, FM 100-5, 2-12 to 2-15.

84 Clive Finkelstein, Information Engineering (Singapore: Addison-Wesley Publishing Company, 1992), 11. Active participation by "managers and users with an expert knowledge of their business...is an essential requirement."

[85] USGAO, Executive Guide, 10.

[86] DA, FM 34-130, Glossary-5 and A-13.

[87] USGAO, Executive Guide, 10.

[88] Ibid.

[89] Department of the Army, Force XXI O&O, *Annex H: Information Operations* [Draft] (Fort Monroe, VA: HQ US Army Training and Doctrine Command, undated), H-1.

[90] See *Annex H* and DA, FM 100-6.

[91] DA, FM 100-6, 1-1. For the current doctrine on the dynamics of combat power, see DA, FM 100-5, 2-10 to 2-12.

[92] See Martin C. Libicki and James A. Hazlett, "Do We Need An Information Corps?" Joint Force Quarterly (Washington, DC: Institute for National Strategic Studies, National Defense University, Autumn 1993/Number 2), 88-97.

[93] Carl Hardeman, Senior Database Advisor, Federal Express Corporation, correspondence with author, 27 Jan 95.

[94] USGAO, Executive Guide, 36.

[95] Daniel P. Bolger, "Command or Control?" Military Review, Volume LXXIV, Number 11 (Fort Leavenworth, KS: US Army Command and General Staff College, July 1990), 69-79. Major Bolger presents a persuasive argument for reducing staff size and reasserting command over control. The information officer should complement this concept, eventually flattening staff structure in a knowledge-based force.

[96] Clausewitz, On War, 95.

[97] DA, TRADOC Pam 525-5, 3-1.

[98] USGAO, Executive Report, 10.

99 Department of the Army, TRADOC Pamphlet 525-5 xx: Concept for Information Operations [Draft] (Fort Monroe, VA: HQ US Army Training and Doctrine Command, undated), 4-4 to 4-6. The Army concept for organization places this officer and attendant staff under the operations officer.

BIBLIOGRAPHY

Books

Allard, C. Kenneth. Command, Control, and the Common Defense. New Haven, CT: Yale University Press, 1990.

Atkinson, Rick. Crusade: The Untold Story of the Persian Gulf War. Boston/New York: Houghton Mifflin Company, 1993.

Bartlett, John. Familiar Quotations. Edited by Emily Morison Beck. Boston, Massachusetts: Little, Brown, and Company, 1980.

Beaumont, Roger A. The Nerves of War: Emerging Issues In and References To Command and Control. Washington, DC: AFCEA International Press, 1986.

Boyes, Jon L. Principles of Command and Control. Washington, DC: AFCEA International Press, 1987.

Braithwaite, Timothy. Information Services Excellence Through TQM: Building Partnerships for Business Process Reengineering and Continuous Improvement. Milwaukee, WI: ASQC Quality Press, 1994.

Campen, Alan D., contributing editor. The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. Fairfax, Virginia: AFCEA International Press, 1992.

Clarkson, Albert. Toward Effective Strategic Analysis: New Applications of Information Technology. Boulder, CO: Westview Press, 1981.

Clausewitz, Carl von. On War. Translated and edited by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Cleveland, Harlan. The Knowledge Executive: Leadership in an Information Society. New York: Truman Talley Books, 1985.

Coakley, Thomas P. C3I: Issues of Command and Control. Washington, DC: National Defense University Press, 1991.

Coakley, Thomas P. Command and Control for War and Peace. Washington, DC: National Defense University Press, 1992.

Cronin, Blaise and Davenport, Elizabeth. Elements of Information Management. Metuchen, NJ: Scarecrow Press, 1991.

Finkelstein, Clive. Information Engineering: Strategic Systems Development. Singapore: Addison-Wesley Publishing Company, 1992.

Johnson, H. Thomas. Relevance Regained: From Top-Down Control to Bottom-Up Empowerment. New York: Free Press, 1992.

Johnson, Stuart E. Science of Command and Control: Coping With Uncertainty. Washington, DC: AFCEA International Press, 1988.

Johnson, Stuart E. Science of Command and Control: Coping With Complexity. Washington, DC: AFCEA International Press, 1989.

Keegan, John. The Mask of Command. New York: Viking, 1987.

Machlup, Fritz. The Study of Information: Interdisciplinary Messages. New York: Wiley, 1983.

Marshall, S.L.A. Men Against Fire: The Problem of Battle Command in Future War. Gloucester, Massachusetts: Peter Smith, 1978.

McKnight, Clarence E. Control of Joint Forces: A New Perspective. Fairfax, VA: AFCEA International Press, 1989.

Meltzer, Morton F. Information, The Ultimate Resource: How to Find, Use, and Manage It. New York: Amacom, 1981.

Munro, Neil. The Quick and the Dead: Electronic Combat in Modern Warfare. New York, St. Martin's Press, 1991.

Roszak, Theodore. The Cult of Information. New York: Pantheon Books, 1986.

Stares, Paul B. Command Performance: The Neglected Dimension of European Security. Washington, DC: Brookings Institution, 1991.

Toffler, Alvin and Heidi. War and Anti-War. Boston/New York: Little, Brown and Company, 1993.

Van Creveld, Martin L. Command in War. Cambridge, MA: Harvard University Press, 1985.

Woodward, Kathleen M. Myths of Information: Technology and Culture. Madison, Wisconsin: Coda Press, 1980.

Zand, Dale E. Information, Organization, and Power. New York: McGraw-Hill Book Company, 1981.

Articles, Manuals, Papers, Projects, and Reports

Bolger, Daniel P. "Command or Control?" Military Review (Volume LXXIV, Number 11, July 1990), 69-79. Fort Leavenworth, KS: US Army Command and General Staff College, 1990.

Condit, Paul D. Principles of Information Resources Management: A Foundation for the Future. Maxwell AFB, AL: Air University Press, 1992.

Cross, Dennis D. Adequacy of Army Airspace Command and Control on the AirLand Battlefield. Carlisle Barracks, PA: US Army War College, 1990.

Cushman, John H. Command and Control of Theater Forces: Issues in Mideast Coalition Command. Cambridge, MA: Harvard University, 1991.

Fallesen, Jon J. Overview of Army Tactical Planning Performance Research. Alexandria, VA: US Army Research Institute, 1993.

Gissin, Raanan. Command, Control, and Communications Technology: Changing Patterns of Leadership in Combat Organizations. Microfiche, 1979.

Hesser, W. Andrew. Force Level Control System Experiment #2: Brigade TOC Information Flows. Springfield, VA: NTIS, 1990.

Hesser, W. Andrew. Commander's Critical Information Requirements and How To Determine Them. Fort Lewis, WA: Pacific Northwest Laboratory, 1991.

Kahan, James F., Worley, Robert D., and Stasz, Cathleen Understanding Commanders' Information Needs. Santa Monica, CA: The RAND Corporation, 1989.

Lesko, John Nicholas. Computer-Based Teleconferencing and its Impact on Command and Control Relationships Within the United States Army. Watertown, MA: US Army Materials Technology Laboratory, 1989.

Libicki, Martin C. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Washington, DC: Institute for National Strategic Studies, National Defense University, 1994.

Libicki, Martin C. and Hazlett, James A. "Do We Need An Information Corps?" Joint Force Quarterly (Autumn 1993/Number 2), 88-97. Washington, DC: Institute for National Strategic Studies, National Defense University, 1993.

Orr, George E. Combat Operations C3I: Fundamentals and Interactions. Maxwell AFB, AL: Air University Press, 1983.

Snyder, Frank M. Command and Control: Readings and Commentary. Cambridge, MA: Harvard University, 1989.

US Congress, Office of Technology Assessment. Informing the Nation: Federal Information Dissemination in an Electronic Age. Washington, DC: US Government Printing Office, 1988.

US, Department of the Army. FM 34-1: Intelligence and Electronic Warfare Operations. Washington, DC: US Government Printing Office, 1994.

US, Department of the Army. FM 34-130: Intelligence Preparation of the Battlefield. Washington, DC: US Government Printing Office, 1994.

US, Department of the Army. FM 100-5: Operations. Washington, DC: US Government Printing Office, 1993.

US, Department of the Army. FM 100-6: Information Operations [Coordinating Draft]. Fort Monroe, VA: HQ US Army Training and Doctrine Command, undated.

US, Department of the Army. TRADOC Pamphlet 525-5: Force XXI Operations. Fort Monroe, VA: HQ US Army Training and Doctrine Command, 1994.

US, Department of the Army. TRADOC Pamphlet 525-xx: Concept for Information Operations (Draft). Fort Monroe, VA: HQ US Army Training and Doctrine Command, undated.

US, Department of the Army. Force XXI O&O, *Annex H: Information Operations* (Draft). Fort Monroe, VA: HQ US Army Training and Doctrine Command, undated.

US, Department of the Army, US Army Computer Science School. IDEF Information Modeling: A Handout/Study Guide. Fort Gordon, AL: US Army Computer Science School, undated.

US, General Accounting Office. Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology. Washington, DC: US General Accounting Office, 1994.

US, General Accounting Office. Information Resources: Summary of Federal Agencies' Information Resources Management Problems. Washington, DC: US General Accounting Office, 1992.

US, General Accounting Office. Information Management and Technology Issues. Washington, DC: US General Accounting Office, 1993.

US, General Services Administration. Managing Office Information Systems in the 1990's. Washington, DC: US General Services Administration, 1989.

Winnefield, James. A. Command and Control of Joint Air Operations: Some Lessons Learned from Four Case Studies of an Enduring Issue. Santa Monica, CA: The RAND Corporation, 1991.